ÖZET

ELEKTRONİK POSTANIN ŞİFRELENMESİNİ SAĞLAYAN BİR SİSTEM

5 Bu buluş, e-posta içeriklerinin kuantum şifreleme teknolojisiyle korunmasını sağlayan bir sistem (1) ile ilgilidir.

İSTEMLER

1. E-posta içeriklerinin kuantum şifreleme teknolojisiyle korunmasını sağlayan;

- e-posta gönderim ve alım süreçlerinde kullanılan verileri organize etmek ve şifreli şekilde depolamak üzere yapılandırılan en az bir kuantum şifreleme modülü (2) içeren ve,
- kuantum şifreleme modülünden (2) alınan şifreli veriler ve meta verilerin, güvenli şekilde şifrelenmesini ve şifrelenmiş e-posta verilerinin yetkisiz erişimlere karşı korunmasını sağlamak üzere yapılandırılan en az bir sunucu (3) ile karakterize edilen bir sistem (1).

2. Herhangi bir iletişim protokolünü kullanarak sunucu (3) ile iletişim kurmak ve veri alışverişi gerçekleştirmek üzere yapılandırılan kuantum şifreleme modülü (2) ile karakterize edilen İstem 1'deki gibi bir sistem (1).

3. Sunucu (3) tarafından yönetilmek üzere yapılandırılan kuantum şifreleme modülü (2) ile karakterize edilen İstem 1 veya 2'deki gibi bir sistem (1).

4. E-posta içeriği, gönderici ve alıcı bilgileri, e-posta başlıkları, tarih ve saat bilgileri, ek dosyalar, şifreleme anahtarları, iletişim protokolü bilgileri ve güvenlik sertifikalarına ait şifreli verileri kayıt altında tutmak üzere yapılandırılan kuantum şifreleme modülü (2) ile karakterize edilen yukarıdaki istemlerden herhangi birindeki gibi bir sistem (1).

5. E-posta gönderim ve alım süreçlerinde kullanılan verileri organize etmek ve şifreli şekilde depolamak üzere yapılandırılan kuantum şifreleme modülü (2) ile karakterize edilen yukarıdaki istemlerden herhangi birindeki gibi bir sistem (1).

6. Herhangi bir iletişim protokolünü kullanarak kuantum şifreleme modülü (2) ile iletişim kurmak ve veri alışverişi gerçekleştirmek üzere yapılandırılan sunucu (3) ile karakterize edilen yukarıdaki istemlerden herhangi birindeki gibi bir sistem (1).

7. Kuantum şifreleme modülünden (2) aldığı şifreli veriler ve meta verileri kuantum anahtar dağıtımı, kuantum gizli paylaşımı, kuantum simetrik şifreleme algoritmaları ile güvenli şekilde şifrelenmesini sağlamak üzere yapılandırılan sunucu (3) ile karakterize edilen yukarıdaki istemlerden herhangi birindeki gibi bir sistem (1).

8. Şifrelenmiş e-posta verilerinin yetkisiz erişimlere karşı korunmasını ve içeriklerin gizliliğini garanti altına alınmasını üzere yapılandırılan sunucu (3) ile karakterize edilen yukarıdaki istemlerden herhangi birindeki gibi bir sistem (1).

TARİFNAME
ELEKTRONİK POSTANIN ŞİFRELENMESİNİ SAĞLAYAN BİR SİSTEM

Teknik Alan

Bu buluş, e-posta içeriklerinin kuantum şifreleme teknolojisiyle korunmasını sağlayan bir sistem ile ilgilidir.

Önceki Teknik

Günümüzde e-posta, hızlı ve etkili bir iletişim aracı olarak yaygın şekilde kullanılmakta ve birçok sektörde veri aktarımı için temel bir araç olarak görevi görmektedir. Mevcut e-posta istemcilerinin kuantum kriptografi sistemleriyle entegre edilmesi, veri güvenliğini önemli ölçüde artırmaktadır. Ancak geleneksel e-posta sistemlerinin düz metin tabanlı yapısı güvenlik açıkları barındırmakta ve bu da verilerin güvenliğini tehlikeye atmaktadır. Bu durum, e-posta içeriklerinin ele geçirilmesi, değiştirilmesi veya posta kutularının tahrip edilmesi gibi risklere yol açmaktadır.

Bu sebeple mevcut teknikte bulunan çalışmalar ve eksiklikler göz önünde bulundurulduğunda kuantum şifreleme teknolojisi kullanarak e-posta verilerinin yüksek güvenlikle şifrelenmesini sağlayan bir sisteme ihtiyaç duyulduğu anlaşılmaktadır.

Tekniğin bilinen durumunda yer alan CN118282626 sayılı Çin patent dokümanında kuantum anahtar şifrelemesine dayalı bir e-posta sisteminden bahsedilmektedir. Söz konusu patent dokümanına konu olan buluş kuantum anahtar şifrelemesine dayalı bir e-posta güvenli aktarım yöntemi ve sistemi sağlamaktadır. Yöntem, kuantum güvenli e-posta bileşenini tanıtarak PSPF teknolojisi temelinde bir e-posta veri paketinin yakalanmasını ve bağımsız şifreleme ve şifre çözme işlemlerini

gerçekleştirmektedir. Kuantum güvenli e-posta bileşeni, e-posta istemcisi ile aynı çalışma ortamında çalıştırılarak gerçekleştirilebilmekte ve e-posta istemcisi ile bağlı olmadan, mevcut e-posta sistemini yükseltmeden veya kullanıcı ağ topolojisini ya da yapısını değiştirmeden uygulanabilmektedir. Kuantum güvenli e-posta bileşeni ve e-posta istemcisi, Outlook, Foxmail gibi yaygın e-posta istemcilerine uygun olup yüksek derecede evrenselliğe sahip bulunmaktadır.

Buluşun Kısa Açıklaması

Bu buluşun amacı, kuantum anahtar dağıtımı yöntemiyle e-posta içeriklerinin güvenli şekilde şifrelenmesini ve yetkisiz erişimlere karşı korunmasını sağlayan bir sistem gerçekleştirmektir.

Buluşun Ayrıntılı Açıklaması

Bu buluşun amacına ulaşmak için gerçekleştirilen “Elektronik Postanın Şifrelenmesini Sağlayan Bir Sistem” ekli şekilde gösterilmiş olup, bu şekil;

Şekil 1 Buluş konusu sistemin şematik görünüşüdür.

Şekilde yer alan parçalar tek tek numaralandırılmış olup, bu numaraların karşılıkları aşağıda verilmiştir:

1. Sistem
2. Kuantum şifreleme modülü
3. Sunucu

E-posta içeriklerinin kuantum şifreleme teknolojisiyle korunmasını sağlayan buluş konusu sistem (1);
- e-posta gönderim ve alım süreçlerinde kullanılan verileri organize etmek ve şifreli şekilde depolamak üzere yapılandırılan en az bir kuantum şifreleme modülü (2) ve,

- kuantum şifreleme modülünden (2) alınan şifreli veriler ve meta verilerin, güvenli şekilde şifrelenmesini ve şifrelenmiş e-posta verilerinin yetkisiz erişimlere karşı korunmasını sağlamak üzere yapılandırılan en az bir sunucu (3) içermektedir.

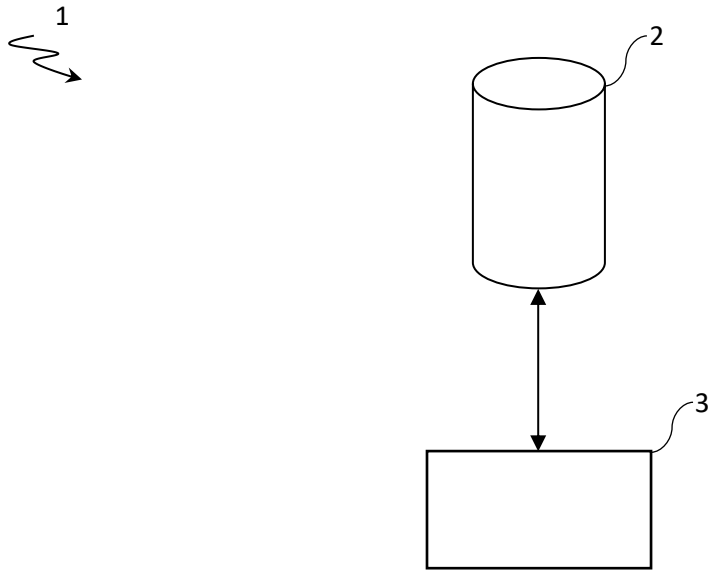
Buluş konusu sistemde (1) yer alan kuantum şifreleme modülü (2), herhangi bir iletişim protokolünü kullanarak sunucu (3) ile iletişim kurmak ve veri alışverişi gerçekleştirmek üzere yapılandırılmaktadır. Kuantum şifreleme modülü (2), sunucu (3) tarafından yönetilmek üzere yapılandırılmaktadır. Kuantum şifreleme modülü (2), e-posta içeriği, gönderici ve alıcı bilgileri, e-posta başlıkları, tarih ve saat bilgileri, ek dosyalar, şifreleme anahtarları, iletişim protokolü bilgileri ve güvenlik sertifikalarına ait şifreli verileri kayıt altında tutmak üzere yapılandırılmaktadır. Kuantum şifreleme modülü (2), e-posta gönderim ve alım süreçlerinde kullanılan verileri organize etmek ve şifreli şekilde depolamak üzere yapılandırılmaktadır.

Buluş konusu sistemde (1) yer alan sunucu (3), herhangi bir iletişim protokolünü kullanarak kuantum şifreleme modülü (2) ile iletişim kurmak ve veri alışverişi gerçekleştirmek üzere yapılandırılmaktadır. Sunucu (3), kuantum şifreleme modülünden (2) aldığı şifreli veriler ve meta verileri kuantum anahtar dağıtımı (QKD), kuantum gizli paylaşımı (QSS), kuantum simetrik şifreleme algoritmaları ile güvenli şekilde şifrelenmesini sağlamak üzere yapılandırılmaktadır. Sunucu (3), şifrelenmiş e-posta verilerinin yetkisiz erişimlere karşı korunmasını ve içeriklerin gizliliğinin garanti altına alınmasını sağlamak üzere yapılandırılmaktadır.

Buluşun Sanayiye Uygulanması

Buluş konusu sistem (1) kuantum anahtar dağıtımı yöntemiyle e-posta verilerinin yüksek güvenlikli şekilde şifrelenmesini sağlayarak, kuantum fiziği prensiplerine dayalı olarak e-posta hizmeti sağlayıcıları, kamu kurumları, finans kuruluşları, sağlık sektörü gibi hassas verilerin korunmasını gerektiren alanlarda sanayide uygulanabilir ve mevcut güvenlik altyapılarına entegre edilerek yüksek risk taşıyan

iletişim süreçlerinde, özellikle gizli ve kritik bilgilerin aktarımı sırasında güvenliği sağlamaktadır.

Bu temel kavramlar etrafında, buluş konusu “Elektronik Postanın Şifrelenmesini Sağlayan Bir Sistem (1)” ile ilgili çok çeşitli uygulamaların geliştirilmesi mümkün olup, buluş burada açıklanan örneklerle sınırlandırılamaz, esas olarak istemlerde belirtildiği gibidir.

Şekil 1